Infotrend

Dedicated Technology Specialists
Providing Innovative **Solutions**

Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning

Request for Information

Solicitation Number:

01234567890

Submission Date:

28 May 2021

Submitted By:

Infotrend, Inc.
301-580-4592
gsingh@infotrend.com
7761 Diamondback Dr
College Park, MD 20742

Section I – Executive Summary

Overview

Department of the Treasury/Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation (FDIC), Bureau of Consumer Financial Protection (CFPB), and National Credit Union Administration (NCUA) issued a request for information from industry on the use of Artificial Intelligence in the commercial industry. Many commercial financial institutions implement artificial intelligence in a multi-step approach by first implementing Robotic Process Automation (RPA) as the stepping-stone and Phase 1 in the intelligent Automation journey. The second stage is adding more sophisticated technologies such as Artificial Intelligence and Machine Learning to be able to address additional capabilities. This implementation is viewed as "Augmented Intelligence" in lieu of Artificial Intelligence. Since it is done through a controlled process leveraging a platform which has the built-in security and auditing to minimize risks. By using this approach, these agencies can begin building the foundation that will enable them to easily transition to Artificial Intelligence and use throughout their institutions.

Intelligent automation is the combination of RPA and cognitive computing technologies such as AI, machine learning, and natural language processing. Software bot capabilities can be expanded beyond the limits of structured data and predefined tasks. Intelligent bots can learn and they can make decisions. In effect, we have moved from programming bots to teaching them. And in some cases, intelligent automation allows our customers to do things that we never thought possible because bots can analyze data so large that humans would not be capable of doing it themselves.

What are the benefits of intelligent automation? According to the Federal News Network survey, 73% of government agency executives said it would move employees away from doing redundant or low-value work. Following that, 60% said it would reduce errors and improve consistency of their missions' outcomes. And 59% said it would supply a better experience to their "customers" (citizens and other agencies). Note that reducing costs came down at the bottom, with just 44%. This shows that perceptions of automation have changed in the marketplace. It is no longer seen as a cost-reducing job killer, but as a job enhancer, and a strategic advantage for agencies.

According to agencies that are in process of implementing intelligent automation, it is good to start first with basic RPA, and then, once you have that mastered, start adding intelligence and cognitive capabilities to it.

The sections below provide a point-by-point response to the Request for Information form the Five (5) Federal Financial Agencies. We believe the responses will provide a better understanding of the value with implementing RPA first before some of the more sophisticated tools such as Artificial Intelligence and Machine Learning. We welcome the opportunity to provide a more in-depth overview of our solution and demos of some of the use cases in Federal.

Question 1: How do financial institutions identify and manage risks relating to AI explainability? What barriers or challenges for explainability exist for developing, adopting, and managing AI?

Industry Response: Robotic Process Automation (RPA) is 100% explainable since it is user-friendly and rules-based, providing transparent audit trails and tracking of all Bot activity. RPA is more powerful from a business automation standpoint when it is paired with AI. In combination, the audit functionality of RPA can be used to track the activity and results from an AI tool. There are many tools available in the world of AI, some of these tools deliver results that are more explainable than others. RPA can collect and correlate the results from multiple tools. This includes results from tools that are less explainable by defining the correlation of the results after performing the automation. This results in greater understanding, greater confidence, and greater trustworthiness. RPA is the key to correlating and tying these tools together intelligently.

Question 2: How do financial institutions use post-hoc methods to assist in evaluating conceptual soundness? How common are these methods? Are there limitations of these methods (whether to explain an AI approach's overall operation or to explain a specific prediction or categorization)? If so, please provide details on such limitations.

Industry Response: Some methods which can only be understood by post hoc analysis, and other methods which are rule-based or experience-based and provide greater explainability can be correlated by RPA automatically to provide greater confidence than post-hoc analysis alone.

Question 3: For which uses of AI is lack of explainability more of a challenge? Please describe those challenges in detail. How do financial institutions account for and manage the varied challenges and risks posed by different uses?

Industry Response: In situations, such as being declined for a mortgage or other type of loan, explainability is more critical since it has a significant impact on customers as well as specific regulatory requirements that must be met. Furthermore, explainable AI enables a sales agent or broker to explain the underlying factors driving their decisions and provide better recommendations leading to better outcomes and a more satisfied customer. Machines do what they do best, to enable humans to do what they do best. A machine could comb through thousands of data results, but the human can do a better job assessing what make sense for the customer. This is one of the driving factors for the release of the Automation Anywhere Robotic Interface (AARI), a solution which allows collaboration between bots and humans.

One example is loan underwriting where the models be unbiased and provide fair results.

Question 4: How do financial institutions using AI manage risks related to data quality and data processing? How, if at all, have control processes or automated data quality routines changed to address the data quality needs of AI? How does risk management for alternative data compare to that of traditional data? Are there any barriers or challenges that data quality and data processing pose for developing, adopting, and managing AI? If so, please provide details on those barriers or challenges.

Industry Response: Most financial institutions have employed Enterprise Data Management frameworks to establish a "single source of the truth" and validate that the data being analyzed is "clean" and can be trusted, as well as to remove duplicates and correct other data quality issues. Sophisticated data management tools are also available to show correlation of and validate the data. For example, knowledge graphs can be leveraged to validate customer identity across social media and other publicly available data sources. RPA can be used to connect to enterprise data management tools and other available data sources (US Census, address data sets, etc..) to ensure that data originates from approved source.

> *Question 5*: Are there specific uses of AI for which alternative data are particularly effective?

Industry Response: Underwriting, KYC/AML compliance, and fraud detection are good use cases. AI can benefit from the use of alternative data in situations where traditional information sources are insufficient or where adding additional dimensions would make recommendations more accurate. In addition, leveraging other data modeling techniques such as knowledge graphs would make the results more accurate.

> *Question 6*: How do financial institutions manage AI risks relating to overfitting? What barriers or challenges, if any, does overfitting pose for developing, adopting, and managing AI? How do financial institutions develop their AI so that it will adapt to new and potentially different populations (outside of the test and training data)?

Industry Response: AI is based on models that are created based on data. In the case of Financial Institutions, AI models are created using the data from the financial institution and continuous feedback learning for these models helps in the models adapting to new and different populations. The biggest challenge is in the data set being used to train AI models which is solved by feedback learning and re-training of models based on what is seen in the real-world environment.

Cybersecurity Risk

Like other data-intensive technologies, AI may be exposed to risk from a variety of criminal cybersecurity threats. For example, AI can be vulnerable to "data poisoning attacks," which attempt to corrupt and contaminate training data to compromise the system's performance.

> *Question 7*: Have financial institutions identified particular cybersecurity risks or experienced such incidents with respect to AI? If so, what practices are financial institutions using to manage cybersecurity risks related to AI? Please describe any barriers or challenges to the use of AI associated with cybersecurity risks. Are there specific information security or cybersecurity controls that can be applied to AI?

Industry Response: Financial institutions utilize several core security frameworks when implementing technologies, regardless of whether they incorporate AI. The security framework follows best practices identified by NIST Cybersecurity Framework. This is to clearly define rules around #1 identify, #2 Protect, #3 Detect, #4 Respond, and #5 Recover. Next, financial institutions educate their employees on best practices and things to be aware of (don't' click on unknown links, and other risks when connected to the network).

They also perform continuous monitoring around the clock and investigate any suspicious activity when detected or reported by an employee. In addition, they assess and manage any potential vulnerabilities uncovered and/or reported incidents. Additionally, they carefully manage third-party risks. Other companies' access to your networks should be scrutinized and limited to ensure this does not create another risk for the financial institution. Lastly, financial institutions utilize Human in the loop automation for AI solutions which can add an extra layer of security and provide data to improve AI models using real world data.

> *Question 8*: **How do financial institutions manage AI risks relating to dynamic updating? Describe any barriers or challenges that may impede the use of AI that involve dynamic updating. How do financial institutions gain an understanding of whether AI approaches producing different outputs over time based on the same inputs are operating as intended?**

Industry Response: It is critical for institutions to establish a Center of Excellence that will govern and provide a framework that oversees and approves AI activities. AI projects should have clear bounds and access limitations to which it must adhere. In addition, regular and agreed upon review of the output data should be performed against the marked objectives of the AI system. This review should be mix of data aggregation with notification triggers, and well as manual review.

> *Question 9:* **Do community institutions face challenges in developing, adopting, and using AI? If so, please provide detail about such challenges. What practices are employed to address those impediments or challenges?**

Industry Response: Smaller institutions face more challenges in implementing AI since they typically have smaller IT teams and more limited technology budgets. As a result, they are more likely to outsource such tools/services. Give the higher risk and lower maturity of many AI solutions, smaller institutions need to perform even more rigorous vetting of their third-party vendors which provide AI-based tools and services, engaging multiple teams across the organization (e.g., technology, risk management, compliance, and vendor management). Risk can also be mitigated by selecting more mature third-party vendors and solutions with a deep financial services customer base.

> *Question 10*: **Please describe any particular challenges or impediments financial institutions face in using AI developed or provided by third parties and a description of how financial institutions manage the associated risks. Please provide detail on any challenges or impediments. How do those challenges or impediments vary by financial institution size and complexity?**

Industry Response: As mentioned above, first and foremost financial institutions need to apply their existing vendor management processes. AI technology is less mature, so the risk is higher. Utilizing AI technologies that are more established, explainable/transparent, and already in use by large financial institutions would minimize risk, especially for smaller institutions.

> **Question 11: What techniques are available to facilitate or evaluate the compliance of AI-based credit determination approaches with fair lending laws or mitigate risks of non-compliance? Please explain these techniques and their objectives, limitations of those techniques, and how those techniques relate to fair lending legal requirements.**

Industry Response: To better protect against built in unfair bias of the AI determination, the model must be heavily scrutinized. This should occur during the COE review of the project as well as from an impartial compliance group. Once approved the bias must be removed before the model is built, by controlling better for sample size of respective groups, as well as thorough testing against available data for potential discrimination. Additionally, financial institutions can now use AI to spot and correct patterns of historic discrimination against minority groups in raw data, adjusting for changes by deliberately altering this data to give an artificial, more equitable probability of approval.

> **Question 12: What are the risks that AI can be biased and/or result in discrimination on prohibited bases? Are there effective ways to reduce risk of discrimination, whether during development, validation, revision, and/or use? What are some of the barriers to or limitations of those methods?**

Industry Response: One potential risk to generating biased AI results is if the data set being utilized is biased, incomplete, or not representative of the demographic being evaluated. In addition, AI tools identify correlations without regarding to the type of input data provided. As such, companies need to tightly govern the data used in AI models is appropriate from a social and regulatory perspective (e.g., ethnicity, gender, etc.) to avoid discrimination.

> **Question 13: To what extent do model risk management principles and practices aid or inhibit evaluations of AI-based credit determination approaches for compliance with fair lending laws?**

Industry Response: Model risk management principles help ensure appropriate data sourcing as well as appropriate governance and controls over the model itself. AI based models require additional scrutiny to ensure that they produce unbiased, explainable results.

> **Question 14: As part of their compliance management systems, financial institutions may conduct fair lending risk assessments by using models designed to evaluate fair lending risks ("fair lending risk assessment models"). What challenges, if any, do financial institutions face when applying internal model risk management principles and practices to the development, validation, or use of fair lending risk assessment models based on AI?**

Industry Response: Financial institution need an extra layer of abstraction to prevent or limit bias. Achieving this, the standardize an algorithm so that it targets not just to fit historical data, but also to score well on some measure of fairness. This is done by including an extra parameter that penalizes the model if it treats protected classes differently.

> **Question 15: The Equal Credit Opportunity Act (ECOA), which is implemented by Regulation B, requires creditors to notify an applicant of the principal reasons for taking adverse action for credit or to provide an applicant a disclosure of the right to request those reasons. What approaches can be used to identify the reasons for taking adverse action on a credit application, when AI is employed? Does Regulation B provide sufficient clarity for the statement of reasons for adverse action when AI is used? If not, please describe in detail any opportunities for clarity.**

Industry Response: AI models can be designed to provide transparency regarding the underlying factors that drive a decision.   Also, at a high-level AI models can be trained to give outputs based on what they see, and these outputs can the information that is given to applicants based on the action taken on their credit.

Additional Considerations

> *Question 16*: **To the extent not already discussed, please identify any additional uses of AI by financial institutions and any risk management challenges or other factors that may impede adoption and use of AI.**

Industry Response:

> *Question 17:* **To the extent not already discussed, please identify any benefits or risks to financial institutions' customers or prospective customers from the use of AI by those financial institutions. Please provide any suggestions on how to maximize benefits or address any identified risks.**

Industry Response: Products, services, and pricing can be better targeted for prospective customer needs. Other potential AI use cases would be in product development to design and deliver personalized products to the market in an accelerated fashion. In addition, financial institutions can use AI in sales and customer service to identify propensity to buy, retention risk, and customer sentiment to better and more quickly meet customer needs.

For the **US Army**, the **business problem** was Contracting officers would manage critical and diverse portfolios of contract requirements for various customers, stakeholders and requiring activities. When a contracting officer completes a contract responsibility determination process, this tedious task could take up to an hour and was required to be done multiple times throughout the entire acquisition process. The Army on average issued approximately 250,000 contracts a year.

The solution was developed and deployed using Automation Anywhere RPA to create the Determination of Responsibility Assistant (DORA) Bot in 2 months. This reduced the amount of time it took Army Contracting Officers to determine contractor responsibility from as much as 2 hours to 2 min saving each contracting officer 312 hours and the US Army as much as $29 million per year. This bot is now being adopted across the DoD as a standard.

Results:	*29M Annual Cost Savings*	*312+ Hours reduced per KO, per year*	*2,184,000 FTE Hours Saved*

For **US Food and Drug Administration (FDA) Centers for Drug Evaluation and Research (CDER)** many employees have pharmaceutical science or medical degrees but find themselves performing repetitive, manual administrative tasks like scheduling meetings and processing intake forms. To market drugs in the U.S. or make changes to their strategy, pharma sponsors must submit their plans to CDER, which is up to thousands of applications per week.

The FDA used RPA for automating drug intake forms and associated processes. Bots ensure applications are complete before transcribing the information in from PDFs into CDER's system. The bots will then determine where to route new drug application, investigation, and master file submissions among hundreds of workflows, so reviewers and project managers have their assignments, and the overall process is exponentially faster and more efficient.

Results in the first six months:	*13,000 Hours reduced*	*24,000 Hours saved*	*34 Processes Automated*	*120+ Bots in Production*

For **FDA Office of Finance** had a high volume of invoice and payments process, both in terms of number of invoices and amount of transactional, manual, and repetitive work required to process them. These processes included highly manual and error-prone tasks. Their vendor payments process also used several disparate IT platforms that do not communicate well with each other.

The FDA used bots to perform the data entry and calculations for each invoice to ensure accuracy and a timely processing of payments. They also used bots that bring together different data points and systems from vendor payments to automate the creation of reports that communicate to the FDA program and acquisition offices. FDA also deployed bots to automate data collection for employee performance metrics associated with the vendor invoice and payment process.

Results:	*500,000 lines of unpaid invoice data processed*	*6000+ hours reduced*

Automation 360

Automation 360

Automation Anywhere released Automation 360 (formerly known as Enterprise A2019) in October 2019. Automation 360 was architected from the ground up to deliver a web-based user experience, it is the latest release of Automation Anywhere's flagship intelligent Digital Workforce platform—offers a choice between on-premises or cloud deployments.

Automation 360 consists of four (4) key components shown below.
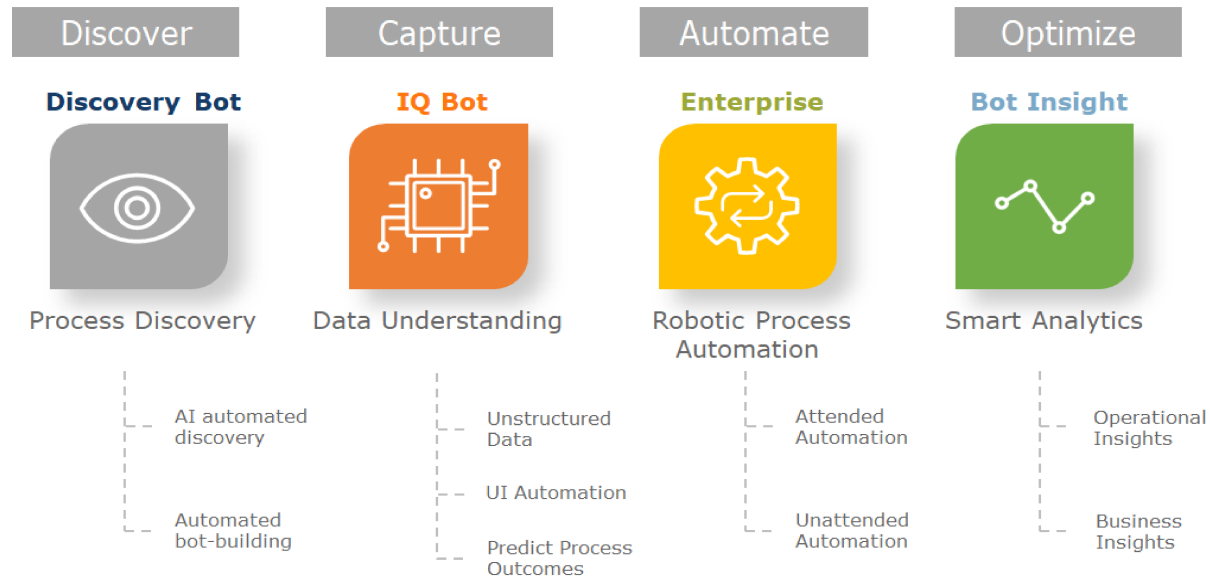
Discovery Bot is one of the components of Automation 360 just recently added to the platform. Discovery Bot provides the ability to determine which processes are the best candidates for automation, their projected ROI, and can provide the automatic creation of those bots.

IQ Bot is the cognitive component of the solution that can extract data from scanned documents or document types where the data fields are in different places each time (eg invoices, Pos). In the area of Capture – the key is data understanding – the ability to recognize unstructured and structured data and pulling it into the platform for use. This is the world of IQ Bot – our leading Intelligent Document Processing solution for this repeatable process.

Robotic Process Automation (RPA) is the core of our automation platform, we view it as Attended, or Unattended automation – that is – whether a human need to be in the loop of the bot that is running. Security comes into play here, as well as governance – must haves for enterprise-grade automation strategies.

Bot Insight is our integrated analytics platform. Our platform-native **Bot Insight** capability enables the data-driven decision making required to optimize bot performance at scale.

Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this document.